Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously Presented) An authentication protocol for increasing safety against a man-in-the-middle computer access attack for point-to-point communication, between a client computer and a server, to services in at least one of a network for data and telecommunication utilizing a challenge-response pattern, comprising:

receiving from a client computer an authentication request containing a clients username to a server providing said services, said server identifying said client computer IP address and client password accessible by the server through the transmitted username;

said server responding with an N byte nonce numerical value;

receiving from said client computer a hash value of at least the parameters clients password, client computer unique IP address, server unique IP address, and said nonce value as an authenticator for accessing said services; and

said server reproducing said authenticator by utilizing said hash algorithm and the parameters clients accessible password, client computer unique IP address, server unique IP address, and said nonce value, comparing the reproduction with the transmitted authenticator, and granting an access to said server and services if said reproduced authenticator matches said transmitted, thus by utilizing said client computer unique IP address and said server unique IP address in said authenticator preventing a man-in-the-middle computer, having a different IP address, from addressing said server with a matching authenticator.

2. (Original) The protocol according to claim 1, wherein said N byte nonce is a random data only generated once by a random generator and used once in said point-to-point communication and then discarded.

3. (Previously Presented) The protocol according to claim 2, wherein the random generator is provided with a seed to produce said nonce numerical value.

4. (Original) The protocol according to claim 3, wherein the seed is comprised of said password and a volatile value.

5. (Original) The protocol according to claim 4, wherein the volatile value is a timestamp value or a counter value.

6. (Original) The protocol according to claim 1, wherein said parameters are concatenated in an arbitrary order before said hash algorithm is applied.

7. (Original) The protocol according to claim 1, wherein said hash algorithm is one of SHA-1, SHA-256, SHA-384 and SHA-512.

8. (Original) The protocol according to claim 1, wherein said hash algorithm is an HMAC utilizing said password as a key.

9. (Original) The protocol according to claim 1, wherein a salt value is concatenated to said password before it is hashed.

10.-21. (Canceled)